New York Law Journal
A NEW YORK LAW JOURNAL SPECIAL SECTION
Cybersecurity
An ALM Publication
WWW.NYLJ.COM
MONDAY, JUNE 6, 2016

Health Care Under (Cyber)attack

With the rise of ransomware and evolving threats, can hospitals ever be prepared?

BY STEVEN J. CHANANIE AND LAURA E. JEHL

By **Steven J. Chananie** | And **Laura E. Jehl**

Remember last year? Experts called 2015 "the year of the health care data breach." The year opened with the news that health insurer Anthem, Inc., had suffered a cyberattack resulting in the theft of personal health information (PHI) for nearly 80 million individuals, including Social Security numbers. The magnitude of the attack, and the sensitive nature of the data stolen from Anthem's systems, sent waves of concern through the health care industry, which had traditionally lagged behind other industries in cybersecurity preparedness. Just six weeks later, the alarm rang again when Premera, a Pacific Northwest health plan, announced that it, too, had suffered a major breach, this time involving the confidential records of 11 million individuals. Next came breaches at CareFirst Blue Cross Blue Shield affecting 1.1 million records, and Excellus, another Blue Cross Blue Shield (BCBS) plan, which disclosed 9 million records. But the health care industry breaches weren't limited to insurers: Hackers broke into UCLA Health System and may have accessed sensitive health information on as many as 4.5 million patients; an attack on Medical Informatics Engineering, a provider of electronic health records, disclosed 3.9 million patient records; and state health agencies in Virginia and Georgia were breached, each disclosing sensitive PHI for hundreds of thousands of individuals. All told, according to the Office for Civil Rights at the Department of Health and Human Services, more than 112 million HIPAA-protected records were disclosed in 2015, the vast majority accessed and/or stolen as a result of cyberattacks.

The health care industry reacted with concern. Historically focused on their compliance obligations under the federal Health Insurance Portability and Accountability Act (HIPAA), insurers, hospitals and other providers had emphasized preventing breaches of patient privacy through the loss or theft of laptops, unauthorized access to patient files by staff, and other inadvertent lapses; by contrast, cybersecurity efforts were often under-funded and unsophisticated. After last year's wave of health care mega-breaches, however, industry players hired teams of forensic security consultants to comb through their electronic data

STEVEN J. CHANANIE *is a partner at Sheppard, Mullin, Richter & Hampton in New York, where he practices in the corporate practice group, focusing on health care issues.* LAURA E. JEHL *is a partner and co-leader of the firm's privacy and data security team in Washington, D.C.*

systems looking for any evidence of compromise, identifying and remediating vulnerabilities, and protecting confidential patient information with encryption. In addition, the Blue Cross and Blue Shield Association announced that all BCBS companies would make identity protection services available to their customers nationwide beginning on or before Jan. 1, 2016, in an effort to provide better safeguards in the event of fraudulent use of customers' personal and financial information.

BIGSTOCK

Still Under Fire?

Fast forward to today, halfway through 2016. Surely it's some other industry's turn in the hacker hot seat, right? Unfortunately, no. While other industries are also under attack, health care continues to bear much of the brunt of cyberattacks. But it's not simply a continuation of 2015's "year of the health care data breach." Instead, experts are calling 2016 "the year of the ransomware attack." This year, the hacker's tool of choice is an increasingly popular form of attack known as "ransomware," which does not steal data but instead disables files and systems by encrypting them with a virtually unbreakable code and demands a payment (the "ransom") to re-enable or unlock them.

In February, for instance, Hollywood Presbyterian, a Los Angeles-area hospital, announced that its communications systems had been disabled for more than a week, until the hospital paid a ransom of 40 bitcoins—about $17,000—and regained access to its systems. And last month, MedStar Health, a 10-hospital system in the Washington, D.C. area, and Prime Healthcare, an operator of three California hospitals, reportedly suffered similar attacks, as did Methodist Hospital in Kentucky. To date, the ransom demands in hospital attacks have not been astronomical—generally, in the tens of thousands of dollars—but the potential threat to patient safety as a result of the disruption of communication and lack of access to patient records has been particularly frightening.

Why is health care still so easily hacked? First, the cybersecurity safeguards of many health care organizations have been aimed at "fighting the last war" rather than anticipating and guarding against new threats. The industry's prior focus on avoiding laptop thefts and unauthorized disclosures of paper files left hospitals and insurers nearly defenseless against last year's sophisticated cyberattacks, which were intended to steal vast troves of electronic data. And now it appears that the emergency—and expensive—remediation efforts undertaken across the industry in response to the 2015 attacks may be inadequate to safeguard those same hospitals against ransomware, a new type of attack.

Many traditional cybersecurity safeguards are simply not aimed

at preventing unauthorized encryption of data and are thus ineffective against ransomware attacks. Although access to systems in both the breach and ransomware scenarios is usually achieved the same way—through "phishing" attacks designed to induce employees to share passwords and/or to download malware—ransomware attacks demand different defenses than cyberattacks intended to steal data. For instance, an important security measure has been the implementation of the encryption of data (and not just during transmission), which renders data unreadable, unusable and unmarketable in the event it is stolen. Such encryption became more widespread, including among many health care companies, following last year's massive breaches. But encryption will not prevent a ransomware attack, since the ransomware itself is not intended to steal data in a meaningfully readable form, but instead itself encrypts the data to make it unreadable and unusable by its rightful owner

Second, despite the advances made in the last year, health care has historically lagged behind other industry sectors in spending on IT security, and may still not have caught up. Third, attacks on the health care industry are financially profitable for hackers. Stolen health care data is often more valuable than stolen credit card data; unlike a credit card, which can be canceled, health care data contains permanent elements such as Social Security numbers which can be used indefinitely to commit identity theft or health care fraud. And ransomware is a low-cost, low-risk cash-generating business for hackers.

And finally, electronic records have been aggressively pushed by the federal and state governments and, as such, embraced by the vast majority of the health care industry as a way to enhance patient care. As a result, hospital staff is more dependent on electronic health records than ever before. If a treating physician can't access critical information such as patient drug dosages, medical history, complex treatment plans or diagnostic tests due to a ransomware attack, treatment can be compromised. Some hospitals that have been attacked have been forced to move temporarily to paper records or to shut down their entire systems for fear of the malware spreading to core servers and functionality.

The impact of a ransomware attack can also extend beyond immediate patient care. Consider, for instance, medical records coders who can't access the records necessary to code for inpatient or outpatient service rendered, thereby preventing the hospital from billing and interrupting the revenue cycle; or a finance department that can't pull up crucial reports, memos or financial data needed to run the hospital day-to-day. Although no ransomware attack to date has been publicly reported to have compromised electronic dosing or treatment systems, such systems, like all computers, can and will eventually be hacked.

Because a ransomware attack has potentially crippling adverse consequences, hospitals are often in an untenable position when facing a ransom demand and, as a result, have been willing to pay the ransom. Experts believe these demands are likely to rise as hackers become more sophisticated about the value of the systems they disrupt, as the attacks themselves become increasingly focused on high value (and high patient-risk) systems, and—importantly—as health care providers become more accustomed to paying ransoms.

And yet unresolved is the question of whether a ransomware attack constitutes a data breach under HIPAA, which defines a breach as the unauthorized "access, acquisition, use or disclosure" of PHI. In most cases, ransomware encrypts—"locks up"—data rather than accessing or disclosing it, leading some experts to argue that there has technically been no breach of PHI, and thus no

reporting requirement under HIPAA. Others view the fact that a system containing PHI came under the control of a hacker, and not the health care provider, as sufficient to constitute a HIPAA violation and require reporting of the attack.

Anticipate the Attack and Prepare Now

Many hospitals have developed sophisticated "enterprise risk management programs" that are designed to address a wide range of institutional risk, from HIPAA privacy and security, to fraud and abuse compliance and disaster preparedness. At the very least, the risk of ransomware attacks should be part of such a program. That includes taking steps to prevent or minimize the occurrence of such attacks, and establishing a clear plan of how to respond to an attack, without panic, and to protect patient safety and the integrity of hospital operations. A copy of this emergency response plan—including phone numbers of key contacts—should be kept somewhere other than on the company's systems.

The best protection against a ransomware attack is frequently and thoroughly backing up all critical applications and data in a secure file, so they can be restored and work properly if an attack cripples the main systems. If a hospital or other victims of a ransomware attack can use its own backups to conduct operations, it's not necessary to pay the ransom, because it can continue operations while the source of the attack is determined. In addition, systems must include robust firewalls. It's crucial that Intrusion Detection/Prevention Systems are up to date and able to receive updates and patches. Hospitals should also consider adopting ransomware-specific detection and prevention systems.

Further, health care providers can benefit from programs to train employees how to recognize phishing attacks. The most effective training sends a series of mock phishing emails to employees who have been told to be on the lookout for attacks. But even the best training is not foolproof; one recent study found that, on average, 13 percent of recipients who received mock emails in training scenarios clicked on a link or opened an attachment associated with the fake phishing email. Administrators should also restrict access to sensitive files and ensure personnel only can access the data necessary to perform their jobs.

Rather than becoming mired in day-to-day demands, or devoting too many scarce resources to "fighting the last war," the health care industry needs to focus on anticipating the next risks on the horizon. Ransomware attacks are likely to become more sophisticated and the attackers savvier about the value of the data they have encrypted, making the potential business impact more devastating. Worse, if hackers choose to devote their efforts toward disabling medical devices and treatment technologies, rather than merely communications systems, the potential risks to patients will skyrocket. Health care's best defense against potentially disastrous future attacks—whether through data breaches, ransomware or the next variant on the horizon—is to be forward-looking, nimble and vigilant.